Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-19 (Cancelled)

20. (Currently Amended) A method for protecting the processing of sensitive information in a security module having a monolithic structure, information processing means, ~~and~~ storage means, distinct from said processing means, for storing information capable of being processed by said processing means, means for checking the integrity of information and at least a data bus, wherein the transmitting of information through said data bus is secured and in that it comprises ~~comprising~~ the following steps:

selecting a piece of sensitive information stored in the storage means;

determining a specific condition for the integrity of said selected information;

reading, by the processing means, of said information ~~and transmitting~~ transmitted from the storage means ~~said information~~ to the processing means for processing via a data bus;

processing said information and verifying, by the processing means or by the means for checking the integrity of information, during the processing that the specific condition is satisfied; and

disabling the processing of said information if the specific condition is not satisfied.

21. (Currently Amended) The method according to claim 20, wherein said information is an operation code read in the storage means, ~~the~~ all of the types of said operation code being contained in a table having a content determined during the manufacture of the security module, and the specific condition for the integrity of the

information being the value of ~~the~~ said information is equal to one of several set values of the table.

22. (Currently Amended) The method according to claim 21, wherein ~~the~~ said operation code to be processed is coded in the form of data bits and said bits do not all have the same binary value.

23. (Currently Amended) The method according to claim 20, wherein the specific step of determining the condition for the integrity of said information comprises ~~checking a calculated~~ calculating a ~~or~~ first piece of integrity data, by means for checking the integrity of information, using ~~said~~ the information read in the storage means, ~~during the reading of said information and transmitting~~ comparing the first piece of integrity data ~~to the processing means, and~~ to ~~calculating~~ a second calculated piece of integrity data by ~~the processing~~ means for checking the integrity of information, using ~~from said~~ the information received by said processing means and checking for equality, by said means for checking the integrity of information, between the first and second pieces of integrity data.

24. (Currently Amended) The method according to claim 23, wherein ~~the first~~ a piece of integrity data is calculated from at least one piece of calculation data whose value varies as a function of time.

25. (Currently Amended) The method according to claim 23, wherein ~~the first~~ a piece of integrity data is calculated from at least one piece of calculation data whose value varies randomly.

26. (Currently Amended) The method according to claim 20, wherein the disabling of the processing of said information is performed by processing means executing a microprogrammed instruction.

27. (Currently Amended) The method according to claim 26, wherein the microprogrammed instruction ~~performs~~ induces the following steps:

writing a piece of disable data into a nonvolatile location of the storage means; and

disabling the processing of ~~said~~ the information.

28. (Currently Amended) The method according to claim 27 further comprising reading by the processing means ~~a~~ said nonvolatile location of the storage means upon power up of said module and disabling the module if a value read at this location does not match.

29. (Currently Amended) A security module comprising an electronic circuit having a monolithic structure and comprising information processing means, ~~and~~ information storage means distinct from said processing means, and means for checking the integrity of information, the processing means ~~means for~~ selecting information extracted from the storage means in order to process it, ~~in said storage means information to be processed and means for extracting selected information from the storage means, said extracting means transmitting said selected information to processing means,~~ the processing means further comprising means for verifying a specific integrity condition of a piece of sensitive information, and means for disabling the processing of the information, said means for disabling being activated when the means for verification or means for checking the integrity of information have detected that the specific condition is not satisfied.

30. (Currently Amended) A security module according to claim 29, wherein the processing means execute instructions corresponding to operation codes extracted from a table, wherein the table comprises at least a forbidden instruction value, the forbidden values being defined during the building of the module.

31. (Currently Amended) A security module according to claim 30, wherein the operation code to be processed is coded in the form of data bits, the security module comprising [[a]] means for reading the values of all the bits and a disabling means activated when the values of the bits are all identical.

32. (Currently Amended) A security module according to claim 29, wherein the processing means execute instructions corresponding to operation codes extracted from a table, the security module comprising [[a]] means for reading an operation code and [[a]] disabling means activated during the reading of a forbidden operation code, the forbidden values being defined during the building of the module.

33. (Currently Amended) A security module according to claim 32, wherein the disabling means comprise [[a]] means for irreversibly writing at least one ~~an~~ indicator with an initial valid state in a non reversible modified invalid state ~~into the storage means~~, and [[a]] means for reading said indicator during the next power-up of the module.

34. (Currently Amended) A security module according to claim 29, wherein means for checking the integrity of information comprise ~~comprising~~ at least one parity ~~generators~~ generator cooperating with the storage means, at least one parity ~~generators~~ generator cooperating with the processing means, and at least one ~~a~~ comparator connected to each of the parity generators and capable of inducing an interrupt in the processing means.

35. (Currently Amended) A security module according to claim 34, wherein the operation of ~~the~~ said parity ~~generators~~ generator varies as a function of time.

36. (Currently Amended) A security module according to claim 34, wherein the operation of ~~the~~ said parity ~~generators~~ generator varies randomly.

37. (Currently Amended) A security module according to claim 33, wherein the irreversible writing of ~~the~~ said indicator ~~into the storage means~~ is performed by executing a microprogrammed instruction.

38. (Previously Presented) A security module according to claim 29, wherein the security module is a microcircuit card.